CA Access Control for Virtual Environments

통합 안내서

r2.0

타사 고지 사항

CONTAINS IBM(R) 32-bit Runtime Environment for AIX(TM), Java(TM) 2 Technology Edition, Version 1.4 Modules

샘플 스크립트와 샘플 SDK 코드

CA Access Control 제품에 포함된 샘플 스크립트와 샘플 SDK 코드는 정보 제공 목적으로만 "있는 그대로" 제공됩니다. 이 항목은 특정 환경에 맞게 수정이 필요할 수 있으며, 프로덕션 환경에 사용하려면 프로덕션 시스템에 배포하기 전에 반드시 테스트 및 검사를 수행해야 합니다.

CA Technologies 는 이러한 샘플에 대한 지원을 제공하지 않으며 이 스크립트로 인한 어떠한 오류에도 책임을 지지 않습니다.

CA 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- CA Access Control Enterprise Edition
- CA Access Control
- [assign the value for UARM in your book]
- CA Identity Manager

설명서 규칙

CA Access Control 설명서는 다음과 같은 규칙을 따릅니다.

형식	의미
고정 폭 글꼴	코드 또는 프로그램 출력
기울임꼴	강조 또는 새 용어
굵게	표시된 대로 동일하게 입력해야 하는 텍스트
슬래시(/)	UNIX 및 Windows 경로를 기술하는 데 사용되는 플랫폼 독립적인 디렉터리 구분 기호

이 설명서는 또한 명령 구문과 사용자 입력(고정 폭 글꼴로 표시됨)을 설명할 때 다음과 같은 특별한 규칙을 사용합니다.

형식	의미
기울임꼴	반드시 입력해야 하는 정보
대괄호([ ]) 사이	선택적 피연산자
중괄호({ }) 사이	필수 피연산자 집합
파이프(|)로 구분된 선택 사항	대체 피연산자(하나 선택)를 구분합니다. 예를 들어, 다음은 사용자 이름 *또는* 그룹 이름 중 *하나*라는 의미입니다. {*username*|*groupname*}

형식	의미
...	앞의 항목 또는 항목 그룹이 반복될 수 있음을 나타냅니다.
밑줄	기본값
줄 마지막에 공백 다음의 백슬래시(\)	때때로 이 안내서에서 명령이 한 줄에 모두 표시되지 않는 경우가 있습니다. 이런 경우에는 줄 끝에 공백과 백슬래시(\)를 표시하여 명령이 다음 줄에서 계속됨을 나타냅니다. **참고:** 실제 명령을 입력할 때는 이러한 백슬래시를 포함하지 말고 줄바꿈 없이 명령을 한 줄에 입력하십시오. 백슬래시 및 줄바꿈은 실제 명령 구문에 포함되지 않습니다.

예제: 명령 표기 규칙

다음 코드는 이 안내서에서 명령 규칙이 사용되는 방식을 보여 줍니다.

ruler *className* [props({all|{*propertyName1*[,*propertyName2*]...})]

설명:

- 표시되는 그대로 입력해야 하는 명령 이름(ruler)은 일반 고정 폭 글꼴로 표시됩니다.
- *className* 옵션은 클래스 이름(예: USER)이 들어갈 자리이므로 기울임꼴로 표시됩니다.
- 대괄호로 묶인 두 번째 부분은 선택적 피연산자를 의미하므로 이 부분 없이 명령을 실행할 수도 있습니다.
- 옵션 매개 변수(props)를 사용할 때 키워드 *all*을 선택하거나 하나 이상의 속성 이름을 쉼표로 구분하여 지정할 수 있습니다.

파일 위치 규칙

CA Access Control 설명서는 다음과 같은 파일 위치 규칙을 따릅니다.

- *ACVEInstallDir* - 기본 CA Access Control for Virtual Environments 설치 디렉터리:
  - /opt/CA/AccessControlServer/VirtualAppliance
- *ACInstallDir* - 기본 CA Access Control 설치 디렉터리입니다.
  - [set the alternate Installation Path variable]
- *ACSharedDir* - UNIX 에서 CA Access Control 에 의해 사용되는 기본 디렉터리입니다.
  - /opt/CA/SharedComponents
- *ACServerInstallDir* - 기본 CA Access Control 엔터프라이즈 관리 설치 디렉터리입니다.
  - /opt/CA/AccessControlServer
- *JBoss_HOME* - 기본 JBoss 설치 디렉터리입니다.
  - /opt/jboss-4.2.3.GA

CA 에 문의

기술 지원팀에 문의

온라인 기술 지원 및 지사 목록, 기본 서비스 시간, 전화 번호에 대해서는 http://www.ca.com/worldwide에서 기술 지원팀에 문의하십시오.

목차

제 1 장: 소개

이 섹션은 다음 항목을 포함하고 있습니다.

안내서 정보

이 안내서는 CA Access Control for Virtual Environments 를 CA 및 타사 제품과 통합하고, 구성하고, 계획하는 방법에 대한 정보를 제공합니다. 또한, 이 안내서는 고가용성 및 재해 복구를 위해 CA Access Control for Virtual Environments 를 계획하고 구성하는 방법에 대한 정보를 제공합니다.

제 2 장: ObserveIT Enterprise 와 통합

이 섹션은 다음 항목을 포함하고 있습니다.

ObserveIT 통합 정보

CA Access Control for Virtual Environments 과 ObserveIT Enterprise 를 통합하면 권한 있는 계정을 사용하여 조직 내 서버에 액세스하려는 시도를 폭넓게 제어할 수 있습니다. ObserveIT Enterprise 세션 로깅 소프트웨어는 대상 시스템에서 사용자의 활동을 기록합니다. 기록은 사용자가 권한 있는 계정 암호를 체크 아웃하고 끝점에 로그인할 때 시작됩니다. 기록은 사용자가 권한 있는 계정 암호를 체크 인할 때처럼 세션이 종료될 때 끝납니다.

기록된 세션은 준비한 전용 데이터베이스에 저장됩니다. ObserveIT 뷰어를 사용하여 CA Access Control 엔터프라이즈 관리에서 직접 기록된 세션을 재생할 수 있습니다.

다음 링크의 ObserveIT Systems 에서 ObserveIT Enterprise 세션 로깅 프로그램을 얻을 수 있습니다.

http://www.observeit-sys.com/download.asp

다음 링크에서 ObserveIT Enterprise 설명서를 찾을 수 있습니다:

https://support.ca.com/cadocs/

참고: ObserveIT 에 대한 자세한 내용은 ObserveIT Enterprise 설치 미디어에 있는 ObserveIT 설명서를 참조하십시오.

통합을 설정하는 방법

여러 단계를 수행하여 CA Access Control for Virtual Environments 를 ObserveIT Enterprise 세션 기록 소프트웨어와 통합합니다. 이 통합의 완료되면 ObserveIT 는 모든 PUPM 세션을 기록합니다.

참고: 1-5 단계를 완료하는 방법에 대한 자세한 내용은 ObserveIT 설치 미디어에 있는 ObserveIT Enterprise 설명서를 참조하십시오.

다음 단계를 수행하십시오.

1. ObserveIT Enterprise 시스템 및 설치 요구 사항을 검토합니다.

   사용하는 서버가 ObserveIT Enterprise 를 설치하기 위한 최소 시스템 요구 사항을 충족하는지 확인합니다.

2. 중앙 데이터베이스를 준비합니다.

   기록된 세션은 전용 Microsoft SQL Server 에 저장됩니다.

3. Internet Information Server(IIS)를 구성합니다.

   ObserveIT Enterprise 응용 프로그램 서버는 IIS 를 사용하여 에이전트가 보내는 메타데이터를 처리합니다.

4. ObserveIT Enterprise 서버 구성 요소를 설치합니다.

   ObserveIT 응용 프로그램 서버, 에이전트, 관리 콘솔도 또한 설치됩니다.

5. ObserveIT Enterprise 응용 프로그램 서버를 구성합니다.

   기록 설정을 구성합니다.

6. 엔터프라이즈 관리 서버에서 세션 기록 스크립트를 배포합니다.

   이 스크립트는 세션 기록을 트리거하는 PUPM 자동 로그인을 활성화합니다.

7. 서비스 계정을 만듭니다.

   사용할 엔터프라이즈 관리 서버에 대한 서비스 계정을 만듭니다.

8. CA Access Control 엔터프라이즈 관리에서 ObserveIT Enterprise 응용 프로그램 서버에 대한 연결을 정의합니다.

   세션 로깅을 사용하도록 연결 설정을 구성합니다.

통합을 준비하는 방법

ObserveIT Enterprise 응용 프로그램 서버의 설치를 완료한 이후에 CA Access Control for Virtual Environments 과의 통합을 위해 서버를 준비합니다. ObserveIT Enterprise 응용 프로그램 서버를 준비하면 서버가 PUPM 세션의 기록 및 저장을 시작하도록 구성됩니다.

다음 단계를 수행하십시오.

1. 관리 콘솔을 엽니다.
2. 서비스 계정을 만듭니다.

   CA Access Control for Virtual Environments 은 서비스 계정을 사용하여 ObserveIT Enterprise 응용 프로그램 서버에 연결합니다.

관리 콘솔을 엽니다.

ObserveIT Enterprise 를 설치 및 시작하면 웹 기반 관리 콘솔을 시작할 수 있습니다.

관리 콘솔을 열려면

1. 브라우저를 사용하여 ObserveIT Enterprise 관리 콘솔을 엽니다. 다음 URL 을 입력합니다.

   http://observeit_server_name:port/ObserveIT

   예:

   http://observeit_server:4884/ObserveIT

2. 설치 시 지정한 administrator 자격 증명을 사용하여 로그인합니다.

   ObserveIT Enterprise 관리 콘솔이 열립니다.

참고: "시작", "프로그램", "ObserveIT", "ObserveIT WebConsole"을 클릭하여 ObserveIT Enterprise 관리 콘솔을 열 수도 있습니다.

서비스 계정 만들기

CA Access Control 엔터프라이즈 관리는 ObserveIT Enterprise 응용 프로그램 서버가 사용자 활동을 기록하도록 인증하기 위해 서비스 계정을 사용합니다. CA Access Control 엔터프라이즈 관리에서 ObserveIT Enterprise 응용 프로그램 서버 연결 설정을 구성할 때 서비스 계정 자격 증명을 제공합니다.

서비스 계정을 만들려면

1. ObserveIT Enterprise 관리 콘솔에서 "Configuration"(구성), "Console Users"(콘솔 사용자)를 선택합니다.

   콘솔 사용자 화면이 열립니다.

2. "Create User"(사용자 만들기)를 선택합니다.

   콘솔 사용자 창이 열립니다.

3. 사용자 이름, 암호를 입력하고 암호를 확인합니다.
4. 인증 방법을 ObserveIT.Authentication 으로 설정하고 사용자 역할을 "Admin"으로 설정합니다.
5. "추가"를 클릭합니다.

   서비스 계정이 만들어졌습니다.

참고: 사용자 관리에 대한 자세한 내용은 ObserveIT Enterprise 설치 미디어에 있는 *ObserveIT 설명서*를 참조하십시오.

세션 기록 스크립트 배포

사용자 세션 기록은 PUPM 자동 로그인과 결합하여 동작합니다. 사용자가 권한 있는 계정 암호를 체크 아웃하고 끝점에 로그인하도록 선택한 경우, 원격 관리 소프트웨어가 열려 자동으로 사용자를 로그인시킵니다. CA Access Control 엔터프라이즈 관리는 끝점 유형을 기반으로 세션 기록 스크립트를 사용하여 원격 관리 프로그램을 제어합니다.

예를 들어, 사용자가 Windows 끝점에 로그인하도록 선택하면 CA Access Control 엔터프라이즈 관리는 끝점에 연결하기 위한 원격 데스크톱 소프트웨어를 엽니다.

ObserveIT Enterprise 응용 프로그램 서버에서 세션을 기록하기 위해 엔터프라이즈 관리 서버에서 세션 기록 스크립트를 배포합니다.

세션 기록 스크립트를 배포하려면

1. CA Support 웹 사이트에서 세션 기록 스크립트를 다운로드하여 임시 디렉터리에 저장합니다.
2. 엔터프라이즈 관리 서버에서 다음 디렉터리로 이동합니다. 여기서 *JBoss_HOME* 은 JBoss 가 설치된 디렉터리를 지정합니다.

   JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/sso_scripts
3. 세션 기록 스크립트를 sso_scripts 디렉터리에 복사합니다.

   덮어쓰기 전에 디렉터리에 있는 파일을 백업하는 것이 좋습니다.
4. 기존 파일을 새 파일로 덮어쓰도록 선택합니다.

이제 연결 설정을 ObserveIT Enterprise 응용 프로그램 서버로 구성할 수 있습니다.

ObserveIT 에 대한 연결 정의

ObserveIT Enterprise 와의 통합을 완료하기 위해 CA Access Control 엔터프라이즈 관리에서 ObserveIT Enterprise 응용 프로그램 서버에 대한 연결 설정을 구성합니다.

ObserveIT 에 대한 연결을 정의하려면

1. CA Access Control 엔터프라이즈 관리에서 "시스템", "연결 관리", "세션 기록", "연결 만들기"를 선택합니다.

   "연결 만들기" 화면이 나타납니다.
2. 다음 세부 정보를 입력합니다.

   연결 설명

   연결의 일반 텍스트 설명을 정의합니다.

   재생 URL

   ObserveIT Enterprise 응용 프로그램 서버 URL 정의

   예:http://observeit_host:4884/observeit/

   사용자 ID

   서비스 계정 사용자 이름 정의

   암호

   서비스 계정 암호 정의

고급

다음 고급 연결 설정을 지정합니다.

뷰어 페이지

세션이 기록되었음을 나타내는 메시지를 화면 맨 위에 표시할지 여부를 지정합니다.

뷰어 매개 변수

ObserveIt 뷰어 창 너비 및 높이를 지정합니다.

ActiveX URL

ObserveIT Enterprise ActiveX 파일이 있는 위치에 대한 전체 경로 이름을 지정합니다. 기본적으로 ObserveIT 응용 프로그램 서버에 대한 URL을 지정합니다.

예:
http://observeit_host:4884/ObserveIT/AgentInstall/Agent.cab#version=1,0,0,0

서버 URL

ObserveIT Enterprise 응용 프로그램 서버가 기록된 세션을 저장하는 위치의 전체 경로 이름을 지정합니다. 기본적으로 ObserveIT 응용 프로그램 서버에 대한 URL을 지정합니다.

예: http://observeit_host:4884/ObserveITApplicationServer

3. "제출"을 클릭합니다.

CA Access Control 엔터프라이즈 관리가 연결을 생성합니다.

제 3 장: PUPM 세션 로깅

이 섹션은 다음 항목을 포함하고 있습니다.

세션이 로깅되는 방법

각 PUPM 세션은 기록되어 ObserveIT Enterprise 데이터베이스에 저장됩니다. 각 세션은 전체 기록된 세션에서 개별적으로 응답할 수 있는 개별 슬라이드로 구분됩니다.

다음 프로세스는 PUPM 세션이 로깅되는 방법을 설명합니다.

1. 사용자가 CA Access Control 엔터프라이즈 관리에서 권한 있는 계정 암호를 체크 아웃하고 끝점에 자동으로 로깅하도록 선택합니다.

   이 옵션을 처음 사용하는 경우 ActiveX 의 설치가 요구됩니다.
2. 원격 관리 세션이 열리고 사용자가 암호를 입력할 필요 없이 로그인됩니다.
3. 끝점에 설치된 ObserveIT 에이전트가 사용자 작업의 기록을 시작하고 슬라이드를 ObserveIT Enterprise 응용 프로그램 서버로 보내면 이 서버가 데이터를 데이터베이스에 저장합니다.
4. 사용자가 원격 관리 세션을 닫고 ObserveIT 에이전트가 기록을 중지합니다.
5. CA Access Control 엔터프라이즈 관리에 기록된 세션이 표시됩니다.

중요! Internet Explorer 가 ActiveX 를 다운로드하도록 활성화하려면 "로컬 인트라넷 영역" 또는 "신뢰할 수 있는 영역"에서 ObserveIT Enterprise 호스트 이름을 지정하고 "서명된 ActiveX 컨트롤 다운로드" 보안 옵션을 "사용"으로 설정하십시오.

참고: 세션 기록에 대한 자세한 내용은 ObserveIT Enterprise 설치 미디어에 있는 *ObserveIT 설명서*를 참조하십시오.

세션이 로깅되는 장소

ObserveIT Enterprise 응용 프로그램 서버는 PUPM 세션을 전용 Microsoft SQL Server 에 로깅합니다. ObserveIT 데이터베이스 서버는 두 개의 전용 데이터베이스를 사용합니다. 첫 번째 데이터베이스의 이름은 ObserveIT 이며, 구성 및 메타데이터를 수록하고 있습니다. 두 번째 데이터베이스의 이름은 ObserveIT_Data 이며, 기록된 세션 중 ObserveIT 에이전트가 수집하는 스크린 샷을 저장합니다.

참고: 세션 로깅에 대한 자세한 내용은 ObserveIT Enterprise 설치 미디어에 있는 *ObserveIT 설명서*를 참조하십시오.

세션 재생

CA Access Control 엔터프라이즈 관리에서 기록된 PUPM 세션을 재생합니다. 세션을 재생하도록 선택하면 CA Access Control 엔터프라이즈 관리가 새 창에서 기록된 세션을 재생합니다. 플레이어 창에는 세션을 탐색하는 데 사용하는 컨트롤 단추가 포함되어 있습니다. 기록된 세션 내에서 일반 텍스트 검색을 수행할 수도 있습니다.

참고: 일반 텍스트 검색에 대한 자세한 내용은 ObserveIT Enterprise 설치 미디어에 있는 *ObserveIT 설명서*를 참조하십시오.

세션을 재생하려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "감사" 하위 작업을 선택합니다.

   사용 가능한 작업의 목록에 "권한 있는 계정 감사" 작업이 나타납니다.

2. "권한 있는 계정 감사"를 선택합니다.

   "권한 있는 계정 감사" 검색 창이 열립니다.

   참고: 자신에게 PUPM 감사 관리자 역할이 할당되어 있는지 확인하십시오.

3. 검색 조건을 지정하고, 표시할 행 수를 입력한 다음 "검색"을 클릭합니다.

   검색 조건에 맞는 작업이 표시됩니다.

4. 세션 정보 열에서 재생 아이콘을 클릭하여 세션을 재생합니다.

   플레이어 창이 열리고 세션의 처음부터 세션이 재생됩니다.

   참고: 세션을 탐색하려면 창의 맨 아래에 있는 컨트롤을 사용하십시오.

제 4 장: 엔터프라이즈 보고 기능 구현

이 섹션은 다음 항목을 포함하고 있습니다.

엔터프라이즈 보고 기능

CA Access Control 엔터프라이즈 관리는 CA Business Intelligence 공용 보고 서버(CA Access Control 보고서 포털)을 통해 보고 기능을 제공합니다. 엔터프라이즈 보고 기능을 사용하면 한 위치에서 각 끝점(사용자, 그룹 및 리소스)의 보안 상태를 볼 수 있습니다. CA Access Control 보고서는 각 끝점에서 누가 무엇을 할 수 있으며 정책 위반이 있는지 여부를 결정하는 규칙 및 정책을 기술합니다.

구성된 이후에 CA Access Control 엔터프라이즈 보고 기능은 독립적으로 실행되어 수동 개입 없이 지속적으로 각 끝점에서 데이터를 수집하여 이 정보를 중앙 서버에 저장합니다. 예약을 통해 또는 요청 시에 각 끝점에서 데이터를 수집할 수 있습니다. 어떤 사용자가 어떤 리소스에 액세스할 수 있는 권한이 있는지 확인하기 위해 각 끝점에 일일이 연결할 필요가 없습니다. 수집 서버가 실행 중인지 여부에 관계없이 각 끝점은 자신의 상태를 보고합니다.

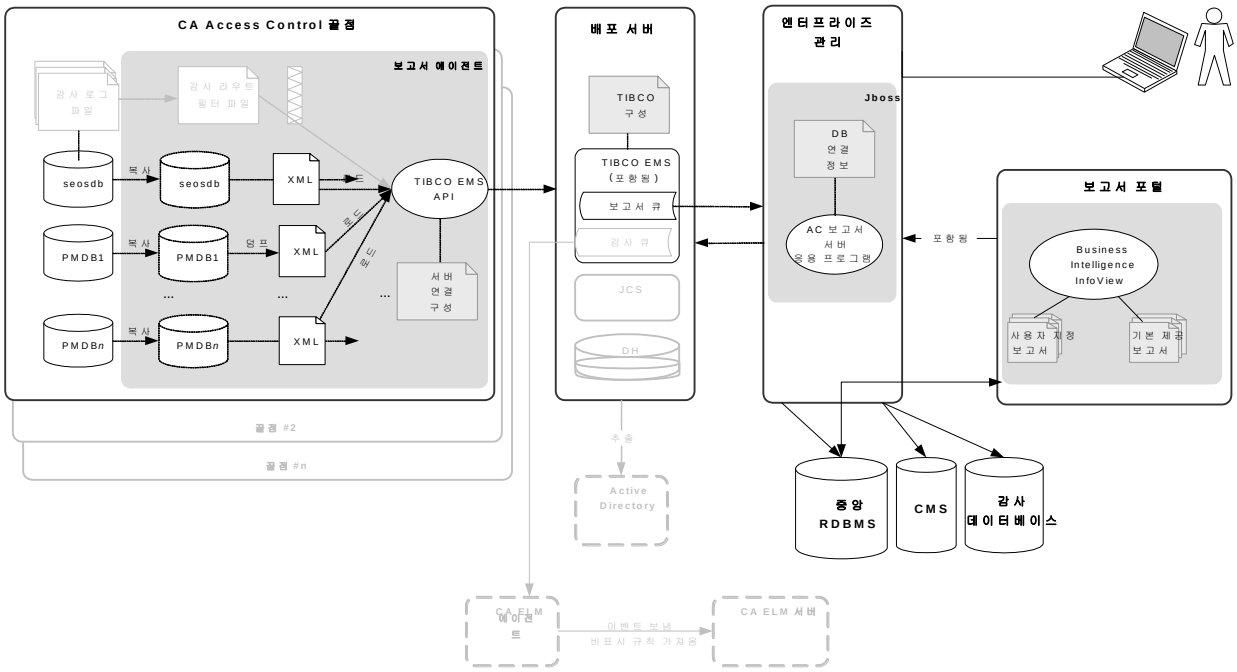
보고 서비스 아키텍처

CA Access Control 보고 서비스는 CA Access Control 엔터프라이즈 보고를 위한 서버 기반 플랫폼을 제공합니다. 이 플랫폼을 사용하여 모든 CA Access Control 끝점의 데이터가 들어 있는 보고서를 작성할 수 있습니다. 작성한 보고서는 웹에서 사용할 수 있는 응용 프로그램을 통해 보고 관리할 수 있습니다.

보고 서비스를 사용하면 기존 CA Access Control 인프라 위에 보고 환경을 구축할 수 있습니다.

참고: 엔터프라이즈 보고에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

다음 다이어그램에서는 보고 서비스 구성 요소의 아키텍처를 보여줍니다. 또한 다음 다이어그램에서는 구성 요소 간의 데이터 흐름을 보여줍니다.



앞의 다이어그램은 다음을 보여줍니다.

- 하나의 CA Access Control 데이터베이스(seosdb)와 임의의 수의 정책 모델(PMDB)이 들어 있는 각 끝점에 보고서 에이전트 구성 요소가 설치되어 있습니다.
- 보고서 에이전트가 끝점에서 데이터를 수집하여 이를 처리하도록 배포 서버로 전송합니다.
- 간단한 엔터프라이즈 모델에서는 하나의 배포 서버를 사용하여 모든 끝점 데이터를 처리하고 중앙 데이터베이스로 보내 저장합니다. 또한 대규모 엔터프라이즈 환경에서 내결함성을 확보하고 처리 성능을 높이기 위해 배포 서버 구성 요소를 복제할 수도 있습니다.
- 중앙 데이터베이스(RDBMS)는 끝점 데이터를 저장합니다.
- 보고서 포털을 사용하면 중앙 데이터베이스의 데이터에 액세스하여 기본 제공 보고서를 만들거나 데이터를 조사하여 사용자 지정 보고서를 만들 수 있습니다.

보고 서비스 서버 구성 요소 설정 방법

엔터프라이즈 보고를 사용하려면 CA Access Control 보고 서비스 서버 구성 요소를 설치 및 구성하십시오. 이 서버 구성 요소를 설치 및 구성한 이후에 각 끝점에서 보고서 에이전트를 구성하십시오.

참고: 보고서 에이전트 설치 및 구성은 CA Access Control 및 [assign the value for unab in your book] 끝점 설치의 일부이며 이 절차에서는 다루지 않습니다.

보고 서비스 서버 구성 요소를 설치하려면 다음 절차를 따르십시오.

1. 이미 수행하지 않은 경우 엔터프라이즈 관리 서버를 설치 및 구성합니다.
2. 보고서 포털 컴퓨터(CA Business Intelligence)를 설정합니다.

   CA Business Intelligence 설치 파일은 CA Support 웹 사이트에서 찾을 수 있습니다.
3. 보고서 포털에 CA Access Control 보고서 패키지를 배포합니다.
4. CA Business Intelligence 에 대한 연결을 구성합니다.
5. 스냅숏 정의를 만듭니다.

   CA Business Intelligence 및 CA Access Control 엔터프라이즈 관리에서 이제 보고서를 생성하고 볼 수 있습니다.

참고: 보고서 생성 및 보기에 대해 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

보고서 포털 컴퓨터를 설정하는 방법

보고서 포털을 사용하면 기본 제공 보고서를 만들거나 데이터를 검색하여 사용자 지정 보고서를 만들기 위해 CA Access Control 엔터프라이즈 관리가 중앙 데이터베이스에 저장하는 끝점 데이터에 액세스할 수 있습니다. 보고서 포털은 CA Business Intelligence 를 사용합니다.

참고: 이전 버전의 보고서 포털이나 독립 실행형으로 설치된 CA Business Intelligence 또는 [assign the value for boe in your book] XI 가 이미 있는 경우 업그레이드할 필요 없이 기존 설치된 제품을 대신 사용할 수 있습니다.

보고서 포털을 설정하려면 다음을 수행하십시오.

1. Oracle 데이터베이스를 사용하는 경우 보고서 포털 컴퓨터에 전체 Oracle 클라이언트를 설치하십시오.
2. Microsoft SQL Server 를 사용하는 경우 보고서 포털 컴퓨터에 Microsoft SQL Server Native Client 를 설치하십시오.
3. 중앙 데이터베이스와 배포 서버를 아직 설정하지 않았으면 지금 설정합니다.

   참고: 엔터프라이즈 관리 서버를 설치할 때 중앙 데이터베이스와 배포 서버를 설정합니다.
4. (UNIX) 보고서 포털 컴퓨터가 Solaris 또는 Linux 컴퓨터인 경우 CA Business Intelligence 설치를 위해 UNIX 컴퓨터를 준비 (페이지 27)합니다.
5. 보고서 포털과 엔터프라이즈 관리 서버의 시스템 시간을 동기화합니다.

   시스템 시간을 동기화하지 않으면 CA Access Control 엔터프라이즈 관리가 생성하는 보고서가 보류 또는 되풀이 상태로 유지됩니다.
6. 사용하는 운영 체제용 CA Business Intelligence 를 설치합니다.

   CA Business Intelligence 설치 파일은 CA Support 웹 사이트에서 찾을 수 있습니다.

   참고: Windows 용 보고서 포털은 기본적으로 Microsoft SQL Server 인증을 사용하여 연결을 인증합니다. 인증을 위해 도메인 사용자 계정 설정을 사용하려면 Windows 인증에서 작업 (페이지 34)하도록 보고서 포털을 구성할 수 있습니다.

   보고서 포털이 설정되고 이제 CA Access Control 보고서 패키지를 배포할 수 있습니다.

참고: CA Business Intelligence 에 대한 자세한 내용은 CA Technologies Support에 있는 *CA Business Intelligence 설치 안내서*를 참조하십시오.

예: Windows 에서 CA Business Intelligence 설치

다음 절차는 Windows 에서 CA Business Intelligence 를 설치하는 절차를 설명합니다.

참고: 설치는 완료될 때까지 약 한 시간 정도 걸릴 수 있습니다.

1. 광 디스크 드라이브에 Windows 용 CA Business Intelligence DVD 를 넣습니다.
2. \Disk1\InstData\VM 폴더로 이동하여 install.exe 를 두 번 클릭합니다.

   CA Business Intelligence 설치 마법사가 시작됩니다.
3. 다음 표를 사용하여 설치 마법사를 완료합니다.

정보	동작
설치 언어	사용할 지원되는 설치 언어를 선택한 다음 "확인"을 클릭하십시오. **참고:** 영어 이외의 지원되는 언어로 설치하려면 현지화(로컬라이제이션)된 운영 체제가 필요합니다.
사용권 계약	"동의함"을 선택한 하고 "다음"을 클릭하십시오.
설치 유형	유형을 선택하고 "다음"을 클릭하십시오.
비 root 자격 증명	비 root 사용자 이름과 암호를 입력하십시오.
BusinessObjects XI 관리자 암호	P@ssw0rd 를 암호 및 암호 확인에 입력한 후 "다음"을 클릭하십시오. **참고:** 암호 규칙에 대한 자세한 내용은 CA Access Control Enterprise Edition 북셸프에 있는 *CA Business Intelligence 설치 안내서*를 참조하십시오.
웹 서버 구성	"다음"을 클릭하여 기본값을 사용하십시오.

정보	동작
CMS 데이터베이스 설정	다음 정보를 입력한 다음 "다음"을 클릭하십시오. ■ **MySQL 루트 암호:** P@ssw0rd ■ **사용자 이름:** cadbusr ■ **암호:** C0nf1dent1al ■ **데이터베이스 이름:** MySQL1 **참고:** CA Business Intelligence 중앙 관리 서버(CMS)는 내부 관리 용도로만 사용됩니다.
감사 사용	"다음"을 클릭하여 기본값을 사용하십시오.
감사 데이터베이스 설정	다음 정보를 입력한 다음 "다음"을 클릭하십시오. ■ **사용자 이름:** cadbusr ■ **암호:** C0nf1dent1al ■ **데이터베이스 이름:** MySQL1
설정 검토	설정을 검토한 다음 "설치"를 클릭하여 설치를 완료하십시오.

설치가 시작되고 완료될 때까지 약 한 시간 정도 걸릴 수 있습니다.

중요! CA Business Intelligence 중앙 관리 서버(CMS)는 내부 관리 용도로만 사용되며 보고서를 생성 및 표시하는 데 사용되는 보고서 데이터를 포함하지 않습니다. CA Access Control 엔터프라이즈 관리를 설치할 때 정의한 보고 데이터베이스는 보고서 에이전트가 배포 서버로 업로드하는 데이터를 포함하고 있습니다. CMS 에 대한 자세한 내용은 *CA Business Intelligence 설치 안내서*를 참조하십시오.

CA Business Intelligence 설치를 위한 Solaris 및 Linux 준비

Solaris 또는 Linux 에 CA Business Intelligence 를 설치하려면 우선 설치를 위해 컴퓨터를 준비해야 합니다. 컴퓨터를 준비할 때 CA Business Intelligence 설치를 위한 비 root 사용자를 만들고, Oracle RDBMS 가 CA Business Intelligence 의 설치를 위해 노출되어 있는지 확인하고, 환경 변수를 설정하십시오.

다음 단계를 수행하십시오.

1. root 사용자로 로그인합니다.
2. 비 root 사용자를 만듭니다. CA Business Intelligence 설치에는 비 root 사용자가 필요합니다.

   예를 들어, 그룹 'other'에 속한 사용자 'bouser'를 만들려면 다음 명령을 입력하십시오.

   ```
   groupadd other
   useradd -d /home/bouser -g other -m -s /bin/bash -c bouser bouser
   passwd bouser
   ```

   메시지가 나타나면 정의한 사용자에 대해 암호를 입력 및 확인합니다.
3. (Linux) LANG 환경 변수가 다음과 같이 구성되었는지 확인합니다.

   ```
   LANG=en US.utf8
   ```
4. 작성한 비루트 사용자로 로그인합니다.
5. ORACLE_HOME 및 TNS_ADMIN 환경 변수가 올바르게 설정되었는지 확인하기 위해 다음 명령을 입력합니다.

   ```
   echo $ORACLE_HOME
   echo $TNS_ADMIN
   ```

   출력이 비어 있지 않으면 이러한 환경 변수가 유효한 것입니다. 예:

   ```
   /opt/oracle/app/oracle/product/10.2.0/client_1
   /opt/oracle/app/oracle/product/10.2.0/client_1/admin/network
   ```

   명령에 대한 출력이 비어 있으면 만든 비 root 사용자에 대해 변수가 설정되어 있는지 확인하십시오. 예를 들면, /home/bouser/.profile 을 다음과 같이 편집합니다.

   ```
   ORACLE_HOME=/opt/oracle/app/oracle/product/10.2.0/client_1
   export ORACLE_HOME
   TNS_ADMIN=$ORACLE_HOME/network/admin
   export TNS_ADMIN
   ```

6. 비루트 사용자에 대한 LD_LIBRARY_PATH 에 다음 경로가 포함되어 있는지 확인합니다.

   $ORACLE_HOME/lib:$ORACLE_HOME/lib32

   예를 들면, 다음 명령을 입력하고 이러한 경로의 출력을 검색합니다.

   echo $LD_LIBRARY_PATH

   이러한 경로가 누락되었으면 이 경로를 LD_LIBRARY_PATH 에 추가합니다. 예를 들면, /home/bouser/.profile 을 다음과 같이 편집합니다.

   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib:$ORACLE_HOME/lib32
   export LD_LIBRARY_PATH

7. LD_LIBRARY_PATH 및 TNS_ADMIN 의 폴더가 액세스 가능한 폴더인지 다음과 같이 확인합니다.

   ls -l $ORACLE_HOME
   ls -l $TNS_ADMIN/tnsnames.ora

   이러한 명령 실행 결과 **사용 권한이 거부되었습니다** 오류가 반환되지 않아야 합니다. 이 오류가 반환될 경우 적절한 권한을 허용해야 합니다. 예를 들어 root/oracle 사용자는 다음 명령을 실행해야 합니다.

   chmod -R +xr $ORACLE_HOME

8. TNS Ping 유틸리티를 사용하여 Oracle 연결이 유효한지 다음과 같이 확인합니다.

   $ORACLE_HOME/bin/tnsping *service_name*

   TNS Ping 의 출력은 다음 예와 유사합니다.

   TNS Ping Utility for Solaris: Version 10.2.0.1.0 - Production on 07-MAY-2008 09:17:02
   Copyright (c) 1997, 2005, Oracle. All rights reserved.
   Used parameter files:
   /opt/oracle/app/oracle/oracle/product/10.2.0/client_1/network/admin/sqlnet.ora
   Used TNSNAMES adapter to resolve the alias
   Attempting to contact (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = 172.16.234.75)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = *service_name*)))
   OK (30 msec)

   이제 Solaris 또는 Linux 에 CA Business Intelligence 를 설치할 수 있습니다.

CA Business Intelligence 설치를 위해 Linux 준비

Linux 에 CA Business Intelligence 를 설치하기 전에 컴퓨터를 준비해야 합니다. 컴퓨터를 준비할 때 CA Business Intelligence 설치를 위한 비 root 사용자를 만들고 환경 변수를 설정합니다.

참고: 사용하는 Linux 버전이 CA Business Intelligence 에서 지원되는지 확인하십시오.

CA Business Intelligence 설치를 위해 Linux 를 준비하려면

1. 비 root 사용자를 만듭니다. CA Business Intelligence 설치에는 비 root 사용자가 필요합니다.

   예를 들어, 사용자 'bouser'를 만들고 암호를 설정하려면 다음 명령을 입력하십시오.

   ```
   useradd -d /home/bouser -m -s /bin/bash -c bouser bouser
   passwd bouser
   ```

2. LANG 환경 변수가 다음과 같이 구성되었는지 확인합니다.

   ```
   LANG=en US.utf8
   ```

보고서 패키지 배포

보고서 패키지는 CA Access Control 표준 보고서를 배포하는 .BIAR 파일입니다. 여기에는 보고서 포털에서의 배포에 대한 아티팩트 및 설명자 모음이 수록되어 있습니다. 이러한 표준 보고서를 사용하려면 보고서 패키지 파일을 BusinessObjects InfoView 로 가져와야 합니다.

참고: 패키지는 보고서 포털의 이전 버전과 호환됩니다. 최신 보고서 패키지를 사용하기 위해 보고서 포털을 업그레이드할 필요는 없습니다. 또한, 별도의 .biar 파일로 제공되는 현지화(로컬라이제이션)된 보고서 패키지를 함께 배포할 수도 있습니다.

보고서 포털에 보고서 패키지 배포

표준 CA Access Control 보고서를 사용하려면 보고서 패키지 파일을 BusinessObjects InfoView 로 가져와야 합니다.

참고: 이 절차는 동일한 패키지의 이전 버전이 이미 배포되지 않은 경우 보고서 포털에서 보고서 패키지를 배포하는 방법을 설명합니다.

다음 단계를 수행하십시오.

1. 중앙 데이터베이스, 배포 서버, 보고서 포털이 설정되었는지 확인합니다.

   참고: 보고서 포털 컴퓨터에서 JAVA_HOME 변수가 설정되었는지 확인합니다.

2. Windows 용 CA Business Intelligence DVD 를 광 디스크 드라이브에 넣고 \Disk1\cabi\biconfig 폴더로 이동합니다.

3. biconfig 디렉터리의 내용을 임시 디렉터리로 복사합니다.

4. 광학 디스크 드라이브에 사용하는 운영 체제용의 적절한 CA Access Control Enterprise Edition 서버 구성 요소 DVD 를 넣은 다음 \ReportPackages 폴더로 이동합니다.

5. 광학 디스크에서 동일한 임시 디렉터리로 다음 파일을 복사합니다.

   - \ReportPackages*RDBMS**import_biar_config*.xml
   - \ReportPackages*RDBMS**AC_BIAR_File*.biar

   RDBMS

   CA Access Control 보고에 사용되는 RDBMS 의 유형을 정의합니다.

   값: Oracle, MSSQL2005

   ***import_biar_config*.xml**

   사용하는 RDBMS 에 대한 가져오기 구성 파일(.xml)의 이름을 정의합니다.

   값: import_biar_config_oracle10g.xml, import_biar_config_oracle11g.xml, import_biar_config_mssql_2005.xml

   참고: 중앙 데이터베이스로 MS SQL Server 2008 을 사용하는 경우 import_biar_config_mssql_2005.xml 파일을 구성하십시오.

   ***AC_BIAR_File*.biar**

   해당 언어 및 RDBMS 의 CA Access Control 보고서 파일(.biar) 이름을 정의합니다.

   참고: 사용하는 RDBMS 에 대한 가져오기 구성 파일의 <biar-file name> 속성은 이 파일을 가리킵니다. 이 속성은 기본적으로 사용하는 RDBMS 의 영어 버전 이름으로 설정되어 있습니다.

6. *import_biar_config*.xml 파일의 사본을 편집합니다. 다음 XML 속성을 정의합니다.

<biar-file name>

CA Access Control 보고서 파일(.biar)에 대한 전체 경로 이름을 정의합니다. 이전 단계에서 이 파일을 복사했습니다.

<networklayer>

사용하는 RDBMS 에서 지원하는 네트워크 계층을 정의합니다.

값(Windows):

- OLE DB - MS SQL Server 인증 모드에 사용
- Oracle OCI
- ODBC - Windows 인증 모드에 사용

값(UNIX): Oracle CLI

<rdms>

CA Access Control 보고에 사용되는 RDBMS 의 유형을 정의합니다.

값(Oracle OCI): Oracle 10 또는 Oracle 11

값(ODBC): 일반 ODBC datasource

값(OLE DB): MS SQL Server 2005, 또는 Oracle 10 또는 Oracle 11 을 *제외*한 임의의 값

참고: MS SQL Server 2008 을 사용하는 경우 이 속성에 대해 MS SQL Server 2005 를 지정하십시오. 이 속성에 대해 지정할 수 있는 값에 대한 자세한 내용은 CA Business Intelligence 설명서를 참조하십시오.

<username>

엔터프라이즈 관리를 위한 중앙 데이터베이스를 준비할 때 만든 RDBMS 관리 사용자의 사용자 이름을 정의합니다.

<password>

엔터프라이즈 관리를 위한 중앙 데이터베이스를 준비할 때 만든 RDBMS 관리 사용자의 암호를 정의합니다.

<datasource>

다음 중 *하나*를 정의합니다.

- (Oracle) 데이터베이스의 이름입니다.
- (SQL Server 2005 또는 2008) 만든 데이터베이스입니다.
- (ODBC) 만든 DSN 입니다.

중요! CA Business Intelligence CMS 가 아니라 보고를 위해 CA Access Control 이 사용하는 데이터베이스의 이름을 지정하십시오.

<server>

SQL Server 2005 또는 2008 컴퓨터의 이름을 정의합니다. Oracle Database 10g, 11g 및 ODBC 에 대해 이 값을 비워두십시오.

7. 다음 작업 중 하나를 수행합니다.

   - (Windows) 명령 프롬프트를 열고 다음 명령을 입력합니다.

     System_Drive:\BO\biconfig.bat -h *host_name* -u *user_name* -p *password* -f *ac_biar_config*.xml

     host_name

     보고서 포털 호스트 이름을 정의합니다.

     user_name

     보고서 포털을 설치할 때 구성한 보고서 포털 관리자를 정의합니다.

     password

     보고서 포털 관리자의 암호를 정의합니다.

     예:

     biconfig.bat -h reportportal.comp.com -u Administrator -p P@ssw0rd -f C:\BO\import_biar_config_oracle11g.xml

   - (UNIX) 스크립트 파일 biconfig.sh 의 실행 권한을 설정하고 다음과 같이 실행합니다.

     temp_dir/biconfig.sh -h *host_name* -u *user_name* -p *password* -f *ac_biar_config*.xml

     예:

     biconfig.sh -h reportportal.comp.com -u Administrator -p P@ssw0rd -f /tmp/rp/import_biar_config_orcl.xml

   배치 파일은 CA Access Control 보고서를 InfoView 로 가져옵니다. 가져오기 작업은 완료될 때까지 몇 분 정도 걸릴 수 있습니다. 배치 파일과 동일한 폴더에 작성된 로그 파일(biconfig.log)은 가져오기의 성공 여부를 나타냅니다.

예: 예제 Oracle Database 11g 가져오기 구성 파일

다음 코드 조각은 Oracle Database 11g 에 대한 편집된 가져오기 구성 파일(import_biar_config_oracle11g.xml)의 예제입니다.

```
<?xml version="1.0"?>
<biconfig version="1.0">
__<step priority="1">
____<add>
______<biar-file name="c:\temp\AccessControl_R12.5_EN_ORCL_22_JUN_2009.biar">
________<networklayer>Oracle OCI</networklayer>
________<rdms>Oracle 11</rdms>
________<username>root</username>
________<password>P@ssw0rd</password>
________<datasource>orcl</datasource>
________<server></server>
______</biar-file>
____</add>
__</step>
</biconfig>
```

예: 예제 Microsoft SQL Server 2005 가져오기 구성 파일

다음 코드 조각은 MS SQL Server 2005 에 대한 편집된 가져오기 구성 파일(import_biar_config_mssql2005.xml)의 예제입니다.

```
<?xml version="1.0"?>
<biconfig version="1.0">
__<step priority="1">
____<add>
______<biar-file name="c:\temp\AccessControl_R12.5_EN_SQL_11_JUN_2009.biar">
________<networklayer>OLE DB</networklayer>
________<rdms>MS SQL Server 2005</rdms>
________<username>dbAdmin</username>
________<password>P@ssw0rd</password>
________<datasource>r125db</datasource>
________<server>rdbms.org</server>
______</biar-file>
____</add>
__</step>
</biconfig>
```

보고서 포털을 위한 Windows 인증 구성

Windows 에 해당

보고서 포털(CA Business Intelligence)을 설치하고 CMS 데이터베이스로 Microsoft SQL Server 를 선택하는 경우, 인증 모드는 SQL Server 인증으로 설정됩니다. Microsoft SQL Server 인증은 SQL 사용자 계정을 사용하여 데이터베이스 연결을 인증합니다.

조직에서 Active Directory 를 사용하는 경우 인증 방법을 Windows 인증으로 수정할 수 있습니다. Windows 인증에서 CMS 데이터베이스에 대한 연결은 로컬 사용자 계정이 아닌 도메인 사용자 계정을 사용하여 인증됩니다.

Windows 인증에서 연결을 인증하면 모든 보고서 포털 구성 요소 사이의 통신 보안을 강화합니다. 사용자 자격 증명을 포함하는 데이터베이스에 대한 ODBC 연결을 구성하므로 보고서 포털에 배포하는 보고서 패키지에서 일반 텍스트 암호를 제거할 수 있습니다.

중요! Windows 인증을 사용하려면 Internet Information Server(IIS)와 Microsoft SQL Server 가 필요합니다.

Windows 인증에서 작업하기 위해 보고서 포털을 구성하는 방법

보고서 포털 데이터베이스 연결 인증 모드를 수정하기 위해 수행하는 단계를 이해하면 Windows 인증에서 보고서 포털을 구현할 때 도움이 됩니다.

Windows 인증을 위한 보고서 포털을 구성하려면 다음을 수행하십시오.

1. CMS 데이터베이스로 사용할 Microsoft SQL Server 2005 데이터베이스를 준비합니다.
2. 기본 사용자 및 데이터 정렬(collation)을 사용하여 CA Business Intelligence CMS 데이터베이스를 준비합니다.
3. 시스템 DSN 을 만들고 SQL Server 인증을 사용하도록 지정합니다.

   보고서 포털 CMS 데이터베이스에 연결하기 위해 시스템 DSN 이 사용됩니다.
4. Active Directory 사용자를 로컬 Administrators 그룹에 추가합니다.

   Windows 인증에서 작업하도록 보고서 포털을 구성할 때 이 사용자를 인증하도록 지정합니다.
5. ASP.NET 웹 서비스 확장이 허용되도록 설정합니다.

6. 보고서 포털CA Business Intelligence (페이지 23)을 설치합니다. 설치 중 다음을 수행하십시오.
   a. 사용자 지정 모드로 CA Business Intelligence 를 설치하도록 선택합니다.
   b. Microsoft SQL Server 2005 를 데이터베이스로 지정합니다.
   c. IIS 를 웹 서버로 지정합니다.
7. Windows 인증에 대해 보고서 포털을 구성합니다.

   Windows 인증에서 인증하기 위해 Active Directory 사용자 계정을 사용하도록 CA Business Intelligence 서비스를 구성합니다.
8. Windows 인증을 사용하여 CA Access Control 보고 데이터베이스에 대한 시스템 DSN 을 만듭니다.

   CA Access Control 보고 포털에 연결하기 위해 시스템 DSN 이 사용됩니다.
9. 보고서 포털에 보고서 패키지를 배포합니다.

Windows 인증을 위한 보고서 포털 구성

보고서 포털을 설치한 다음에는 Windows 인증에서 작업하도록 보고서 포털을 구성할 수 있습니다. Active Directory 사용자 계정을 사용하도록 보고서 포털을 구성하고 시스템 DSN 연결 매개 변수를 수정합니다.

Windows 인증을 위한 보고서 포털을 구성하려면

1. 운영 체제 관리자로 보고서 포털 호스트에 로그인합니다.
2. 보고서 포털 CMS 에 대한 시스템 DSN 을 Windows NT 인증으로 수정합니다.
3. "시작", "프로그램", "BusinessObjects XI Release 2", "Business Objects Enterprise", "Central Configuration Manager"를 차례로 선택합니다.

   Central Configuration Manager 가 열리고 CA Business Intelligence 서비스가 표시됩니다.
4. 모든 CA Business Intelligence 서비스를 중지합니다.
5. 서비스 "Log On As" 설정을 Active Directory 사용자 자격 증명으로 수정합니다. 모든 CA Business Intelligence 서비스에 대해 이 작업을 수행하십시오.

   중요! "WinHTTP Web Proxy Auto-Discovery" 및 "World Wide Web Publishing" 서비스의 설정을 변경합니다.
6. 모든 CA Business Intelligence 서비스를 시작합니다.

   보고서 포털이 이제 Windows 인증에서 인증하도록 구성되었습니다.

   참고: Microsoft SQL Server 작업 모니터에서 보고 데이터베이스에 대한 연결이 Active Directory 사용자 계정을 사용함을 확인할 수 있습니다.

예: CA Business Intelligence 서비스 "Log On As" 연결 설정 수정

다음 예는 CA Business Intelligence 연결 서버 서비스 "Log On As" 자격 증명을 시스템 계정에서 Active Directory 계정으로 수정하는 방법을 설명합니다.

1. 목록에서 "Connection Server" 서비스를 마우스 오른쪽 단추로 클릭하고 "Properties"를 선택합니다.

   "Connection Server" 서비스 속성 창이 열립니다.

2. "Log On As" 섹션에서 "System Account" 옵션의 표시를 제거합니다.

   연결 설정 필드가 활성화됩니다.

3. Active Directory 사용자 이름, 암호를 입력하고 암호를 확인합니다.

   예: Domain/username

   "확인"을 클릭합니다. 서비스 연결 설정이 변경되었습니다.

4. Central Configuration Manager 를 종료합니다.

시스템 DSN 연결 구성 예제

시스템 DSN 연결 설정은 데이터베이스에 연결하기 위해 필요한 매개 변수를 정의합니다. 다음 예에서는 보고서 포털이 설치되었을 때 SQL 인증만 지원하므로 SQL Server 서버 인증에서 사용자 연결을 인증하는 시스템 DSN 을 만듭니다. CA Business Intelligence 를 설치하기 전에 CMS 데이터베이스 시스템 DSN 을 구성합니다.

다음 예에서는 보고서 포털 CMS 데이터베이스에 대한 시스템 DSN 을 만듭니다.

1. "시작", "설정", "제어판", "관리 도구", "데이터 원본 (ODBC)"를 차례로 선택합니다.

   ODBC 데이터 원본 관리자가 열립니다.

2. "시스템 DSN" 탭에서 "만들기"를 선택합니다.

   "새 데이터 원본 선택" 창이 열립니다.

3. 아래로 스크롤하여 "SQL Server"를 선택한 다음 "마침"을 클릭합니다.

   "SQL Server 에 새로운 데이터 원본 만들기" 마법사가 열립니다.

4. 연결 이름, 설명, SQL 서버 이름을 입력합니다. "다음"을 클릭합니다.
5. SQL Server 인증을 사용하도록 선택합니다.
6. SQL 서버에 연결하기 위한 administrator 사용자 자격 증명을 입력합니다. "다음"을 클릭합니다.
7. "기본 데이터베이스를 다음으로 변경" 옵션을 선택하고 목록에서 보고서 포털 CMS 데이터베이스를 선택합니다. "다음"을 클릭합니다.
8. "마침"을 클릭합니다. 연결을 테스트하도록 선택하고 "확인"을 클릭합니다.

   시스템 DSN 이 생성되었습니다.

Windows 인증에서 작업하는 보고서 포털에 보고서 패키지 배포

Windows 에 해당

이러한 표준 CA Access Control 보고서를 사용하려면 보고서 패키지 파일을 BusinessObjects InfoView 로 가져와야 합니다.

참고: 이 절차는 동일한 패키지의 이전 버전이 이미 배포되지 않은 경우 보고서 포털에서 보고서 패키지를 배포하는 방법을 설명합니다.

보고서 포털에 보고서 패키지를 배포하려면

1. 중앙 데이터베이스, 배포 서버, 보고서 포털이 설정되었는지 확인합니다.

   참고: 보고서 포털 컴퓨터에서 JAVA_HOME 변수가 설정되었는지 확인합니다.

2. CA Access Control 보고 데이터베이스에 대한 시스템 DSN 을 만들고 Windows NT 인증을 사용하도록 지정합니다.

   만드는 시스템 DSN 은 CA Access Control 보고 데이터베이스에 연결하는 데 사용됩니다. 보고서 패키지를 구성할 때 시스템 DSN 을 지정합니다.

3. Windows 용 CA Business Intelligence DVD 를 광 디스크 드라이브에 넣고 \Disk1\cabi\biconfig 폴더로 이동합니다.

4. biconfig 디렉터리의 내용을 임시 디렉터리로 복사합니다.
5. 광학 디스크 드라이브에 사용하는 운영 체제용의 적절한 CA Access Control Enterprise Edition 서버 구성 요소 DVD 를 넣은 다음 \ReportPackages 폴더로 이동합니다.
6. 광학 디스크에서 동일한 임시 디렉터리로 다음 파일을 복사합니다.
   - \ReportPackages*RDBMS**import_biar_config*.xml
   - \ReportPackages*RDBMS**AC_BIAR_File*.biar

   RDBMS

   CA Access Control 보고에 사용되는 RDBMS 의 유형을 정의합니다.

   값: MSSQL2005

   ***import_biar_config*.xml**

   사용하는 RDBMS 에 대한 가져오기 구성 파일(.xml)의 이름을 정의합니다.

   값: import_biar_config_mssql_2005.xml

   참고: 중앙 데이터베이스로 MS SQL Server 2008 을 사용하는 경우 import_biar_config_mssql_2005.xml 파일을 구성하십시오.

   ***AC_BIAR_File*.biar**

   해당 언어 및 RDBMS 의 CA Access Control 보고서 파일(.biar) 이름을 정의합니다.

   참고: 사용하는 RDBMS 에 대한 가져오기 구성 파일의 <biar-file name> 속성은 이 파일을 가리킵니다. 이 속성은 기본적으로 사용하는 RDBMS 의 영어 버전 이름으로 설정되어 있습니다.
7. *import_biar_config*.xml 파일의 사본을 편집합니다. 다음 XML 속성을 정의합니다.

   중요! 파일에서 사용자 이름, 암호, 서버 필드를 제거하십시오.

   <biar-file name>

   CA Access Control 보고서 파일(.biar)에 대한 전체 경로 이름을 정의합니다. 이 파일은 이전 단계에서 복사한 파일입니다.

   <networklayer>

   사용하는 RDBMS 에서 지원하는 네트워크 계층을 정의합니다.

   값: ODBC

<rdms>

CA Access Control 보고에 사용되는 RDBMS 의 유형을 정의합니다.

값: 일반 ODBC 데이터 원본

<datasource>

만든 DSN 을 정의합니다.

중요! CA Business Intelligence CMS 가 아니라 보고를 위해 CA Access Control 이 사용하는 데이터베이스의 이름을 지정하십시오.

8. 명령 프롬프트 창을 열고 다음 명령을 입력합니다.

System_Drive:\BO\biconfig.bat -h *host_name* -u *user_name* -p *password* -f *ac_biar_config*.xml

host_name

보고서 포털 호스트 이름을 정의합니다.

user_name

보고서 포털을 설치할 때 구성한 보고서 포털 관리자를 정의합니다.

password

보고서 포털 관리자의 암호를 정의합니다.

예:

biconfig.bat -h reportportal.comp.com -u Administrator -p P@ssw0rd -f C:\BO\import_biar_config_mssql_2005.xml

예: Windows 인증을 사용하도록 구성된 예제 Microsoft SQL Server 2005 가져오기 구성 파일

다음 코드 조각은 Windows 인증에서 작업하는 보고서 포털에 배포하는 MS SQL Server 2005 에 대한 편집된 가져오기 구성 파일(import_biar_config_mssql2005.xml)의 예제입니다.

```
<?xml version="1.0"?>
<biconfig version="1.0">
        <step priority="1">
                <add>
                        <biar-file name="c:\temp\biconfig\
                        AccessControl_R12.5_EN_JP_KR_SQL_6_DEC_2009.biar">
                                <networklayer>ODBC</networklayer>
                                <rdms>Generic ODBC datasource</rdms>
                                <datasource>acdb</datasource>
                        </biar-file>
                </add>
        </step>
</biconfig>
```

대규모 배포를 위한 BusinessObjects 구성

대규모 배포에서 CA Access Control 보고서를 실행하려면 BusinessObjects 기본 구성을 변경해야 합니다. BusinessObjects 페이지 서버에서 허용되는 최대 동시 연결 수(기본값: 20,000)를 변경할 수 있습니다. 또한 입력 매개 변수 선택 목록에 표시된 값의 최대 수를 변경합니다.

대규모 배포를 위해 BusinessObjects 를 구성하려면

1. BusinessObjects 페이지 서버가 연결할 수 있는 동시 연결 수를 변경합니다.
   a. 보고서 포털 컴퓨터에서 "시작", "프로그램", "Crystal Enterprise", "Crystal Configuration Manager"를 클릭합니다.

      BusinessObjects 구성 매니저가 열립니다.

   b. Crystal 페이지 서버를 마우스 오른쪽 버튼으로 클릭한 다음 "중지"를 선택합니다.

   c. Crystal 페이지 서버를 마우스 오른쪽 버튼으로 클릭한 다음 "속성"을 선택합니다.

d. "실행 파일" 경로 필드의 *-restart* 뒤에 다음 텍스트가 표시되는지 확인합니다.

-maxDBResultRecords 0

e. BusinessObjects 페이지 서버를 다시 시작합니다.

2. 보고서의 입력 매개 변수 선택 목록에 표시된 값의 최대 수를 변경합니다.

a. Windows 레지스트리 편집기를 엽니다.

b. 다음 레지스트리 키를 탐색합니다.

HKEY_CURRENT_USER/Software/Business Objects/Suite 11.5/Crystal Reports/Database

c. "편집", "새로 만들기", "DWORD 값"을 클릭합니다.

REG_DWORD 유형의 새 레지스트리 항목이 나타납니다.

d. 항목의 이름을 *QPMaxLOVSize* 로 지정합니다.

e. 항목을 두 번 클릭하고 그 값의 데이터를 1000 으로 편집합니다.

새 레지스트리 항목이 설정됩니다.

f. BusinessObjects CMC(Central Management Console-중앙 관리 콘솔)를 엽니다.

g. 서버 관리 영역으로 이동합니다.

h. 설정을 변경할 웹 인텔리전스 보고서 서버를 클릭합니다.

"웹 인텔리전스 보고서 서버" 페이지가 "속성" 탭에 열립니다.

i. 다음 값을 1000 이상 또는 요구된 값으로 수정합니다.

- 값 배치 크기 목록
- 사용자 지정 정렬 값의 최대 목록 크기

변경 내용을 제출하려면 "적용"을 클릭하고 변경 내용의 효력이 즉시 발생할 수 있도록 서버를 다시 시작합니다.

CA Business Intelligence 에 대한 연결 구성

CA Access Control 엔터프라이즈 관리는 CA Business Intelligence 공용 보고 서버(CA Access Control 보고서 포털)을 통해 보고 기능을 제공합니다. 보고서 포털을 설치하고 보고서를 배포한 다음에는 CA Access Control 엔터프라이즈 관리에서 CA Business Intelligence 로의 연결을 구성해야 합니다. 이 연결을 구성하려면 CA Identity Manager 관리 콘솔을 사용합니다.

CA Business Intelligence 에 대한 연결을 구성하려면

1. CA Identity Manager 관리 콘솔을 활성화합니다.
2. CA Identity Manager 관리 콘솔을 엽니다.
3. "환경", "AC 환경", "고급 설정", "보고서"를 차례로 클릭합니다.

   "보고서 속성" 창이 나타납니다.
4. 데이터베이스 및 Business Objects 속성을 입력합니다.

   중요! CA Business Intelligence 중앙 관리 서버(CMS)는 내부 관리 용도로만 사용되며 보고서를 생성 및 표시하는 데 사용되는 보고서 데이터를 포함하지 않습니다. CMS 에 대한 자세한 내용은 *CA Business Intelligence 설치 안내서*를 참조하십시오.

   참고: 자세한 내용은 제품에 포함된 *CA Identity Manager 관리 콘솔 온라인 도움말*을 참조하십시오.

   중요! "Business Objects 포트" 필드에서 보고서 포털이 사용하는 포트 번호를 입력하십시오. 기본 포트는 8080 입니다. "Business Objects 보고서 폴더" 필드에 "CA Access Control r12"를 입력합니다.
5. "저장"을 클릭합니다.

   CA Business Intelligence 설정이 저장됩니다.

참고: CA Business Intelligence 에 대한 자세한 내용은 CA Technologies Support에 있는 *CA Business Intelligence 설치 안내서*를 참조하십시오.

스냅숏 정의 만들기

보고서는 CA Access Control 및 [assign the value for unab in your book] 끝점에서 수집하여 중앙 데이터베이스에 저장된 데이터 스냅숏, CA Access Control 엔터프라이즈 관리의 PUPM 데이터, 사용자 저장소의 데이터에 기반합니다.

CA Access Control 보고서를 실행하고 보려면 먼저 스냅숏 정의를 만들고 스냅숏 데이터를 캡처합니다. 스냅숏 정의는 CA Access Control 이 수집하는 보고서 데이터와 데이터 수집을 위한 일정을 지정합니다.

스냅숏 매개 변수 XML 파일은 CA Access Control 이 수집하는 보고서 데이터를 지정합니다. 기본적으로 이 파일은 모든 CA Access Control 및 [assign the value for unab in your book] 끝점, PUPM 데이터, 보고서 스냅숏의 사용자 저장소에 있는 데이터를 포함하도록 지정합니다. 보고서 스냅숏의 범위를 제한하도록 스냅숏 매개 변수 XML 파일을 사용자 지정할 수 있습니다.

보고서에 가장 최신 데이터가 수록되도록 끝점 스냅숏보다 더 자주 스냅숏이 실행되도록 예약하지 마십시오. 예를 들어, 끝점이 매주 스냅숏을 보내도록 구성하고 CA Access Control 엔터프라이즈 관리가 매일 스냅숏을 캡처하도록 구성하면 보고서 데이터가 끝점에서는 매주 수집되지만 PUPM 및 사용자 저장소에서는 매일 수집되어 보고서에 오래된 끝점 데이터가 표시됩니다.

중요! 여러 스냅숏 정의를 활성화하지 마십시오. 여러 스냅숏 정의가 활성화된 경우 CA Access Control 엔터프라이즈 관리는 모든 보고서를 성공적으로 실행할 수 없습니다.

참고: 기본적으로 스냅숏 정의를 만들려면 시스템 관리자 역할이 있어야 합니다.

스냅숏 정의를 만들려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "보고서"를 클릭합니다.
   b. "작업" 하위 탭을 클릭합니다.
   c. 작업 메뉴에서 왼쪽에 있는 "스냅숏 정의 관리" 트리를 확장합니다.

      사용할 수 있는 작업 목록에 "스냅숏 정의 만들기" 작업이 나타납니다.
2. "스냅샷 정의 만들기"를 클릭합니다.

   "스냅숏 정의 만들기: 스냅숏 정의 선택" 페이지가 나타납니다.
3. "확인"을 클릭합니다.

   "스냅숏 정의 만들기" 페이지가 나타납니다.
4. "프로필" 탭에서 다음 필드를 완성합니다.

   스냅숏 정의 이름

   스냅숏 정의의 이름을 정의합니다.

   스냅숏 정의 설명

   스냅숏 정의를 설명하는 추가 정보를 지정합니다.

   사용

   CA Access Control 엔터프라이즈 관리가 스냅숏 정의를 활성화하도록 지정합니다.

   참고: 이 확인란을 선택하지 않으면 CA Access Control 엔터프라이즈 관리가 스냅숏을 캡처하지 않으며 보고서가 표시되지 않습니다. 스냅숏은 한 번에 하나씩만 활성화할 수 있습니다.

식별자

보고서 스냅숏의 범위를 정의하는 스냅숏 매개 변수 XML 파일을 지정합니다.

기본값: PPM_ALL.xml

마지막 유지

중앙 데이터베이스에 저장된 성공한 스냅숏의 수를 지정합니다. CA Access Control 은 데이터베이스에 있는 스냅숏의 수가 지정된 수에 도달하면 오래된 스냅숏을 삭제합니다.

참고: 스냅숏 수는 0 보다 커야 합니다. 이 필드의 값을 지정하지 않으면 CA Access Control 은 스냅숏을 무제한 저장합니다. 최대 3 개의 성공한 스냅숏을 저장하는 것이 좋습니다.

5. "되풀이" 탭을 클릭하고 "일정"을 선택합니다.

   일정 옵션이 나타납니다.

6. 스냅숏 실행 시간 및 되풀이 패턴을 지정하고 "제출"을 클릭합니다.

   참고: CA Access Control 및 [assign the value for unab in your book] 끝점의 스냅숏보다 덜 자주 스냅숏이 실행되도록 예약하는 것이 좋습니다.

   CA Access Control 은 예정된 시간 및 빈도로 스냅숏을 캡처하도록 구성되었습니다.

참고: 스냅숏 정의를 만든 이후에 필요할 때 스냅숏을 캡처하거나 예약된 시간 및 빈도로 스냅숏을 캡처하도록 선택할 수 있습니다. 스냅숏 데이터 캡처에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

보고서 스냅숏의 범위 제한

CA Access Control 엔터프라이즈 관리가 보고서 스냅숏을 캡처할 때는 CA Access Control 및 [assign the value for unab in your book] 끝점의 스냅숏에서 데이터를 수집하고, CA Access Control 엔터프라이즈 관리에서 PUPM 데이터를 수집하고, 사용자 저장소에서 데이터를 수집합니다. CA Access Control 엔터프라이즈 관리가 보고서 데이터를 수집한 다음에는 이 데이터를 중앙 데이터베이스에 저장합니다.

스냅숏 매개 변수 XML 파일은 CA Access Control 엔터프라이즈 관리이 수집하는 보고서 데이터를 지정합니다. 스냅숏 매개 변수 XML 파일을 사용자 지정하여 보고서 스냅숏의 범위를 제한할 수 있습니다.

예를 들어, 사용자 저장소로 Active Directory 를 사용하는 경우, CA Access Control 엔터프라이즈 관리는 보고서 스냅숏을 캡처할 때 모든 Active Directory 사용자에 대한 데이터를 수집합니다. 이 작업은 완료하는 데 시간이 오래 걸릴 수 있습니다. 스냅숏을 캡처하는 데 걸리는 시간을 줄이려면 스냅숏 매개 변수 XML 파일을 사용자 지정하여 Active Directory 스냅숏의 범위를 제한할 수 있습니다.

보고서 스냅숏의 범위를 제한하려면

1. 다음 디렉터리로 이동합니다. 여기서 *JBOSS_HOME* 은 JBoss 를 설치한 디렉터리를 나타냅니다.

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/imrexport/sample

2. PPM_ALL.xml 파일을 복사하고, 새 파일의 이름을 변경하고, 파일을 동일한 디렉터리에 저장합니다.

   새 스냅숏 매개 변수 XML 파일을 만들었습니다.

3. 편집 가능한 형식으로 새 스냅숏 매개 변수 XML 파일을 엽니다.

4. <!--IM COLLECTORS--> 섹션의 항목을 편집하여 CA Access Control 엔터프라이즈 관리가 사용자 저장소에서 수집하는 데이터의 범위를 지정합니다.

5. 보고서 스냅숏에 포함하고 싶지 않은 CA Access Control 엔터프라이즈 관리 구성 요소에 해당하는 <!--PUPM COLLECTORS--> 섹션의 항목을 주석 처리(!-- 및 --)합니다.

6. (선택 사항) Active Directory 스냅숏의 범위를 제한합니다.

   a. LDAP 쿼리가 보고서 스냅숏을 제한하는 방법 (페이지 54)과 LDAP 구문 고려 사항 (페이지 55) 항목을 검토합니다.

      이 항목의 정보는 다음 단계를 통해 올바른 LDAP 쿼리를 정의하는 데 도움을 줍니다.

   b. <!--PUPM COLLECTORS--> 섹션에서 다음 요소를 찾습니다.

      ```
      <export object="com.ca.ppm.export.ADUsersCollector">
      </export>
      ```

      이 요소는 스냅숏에 포함된 Active Directory 사용자 데이터를 지정합니다.

   c. 다음과 같이 보이도록 이 요소를 편집합니다. 여기서 *ldap_query* 는 데이터가 수집된 대상 사용자를 정의하는 LDAP 쿼리를 지정합니다.

      ```
      <export object="com.ca.ppm.export.ADUsersCollector">
              <where attr="%USER" satisfy="ANY">
                      <value op="EQUALS">(ldap_query)</value>
              </where>
      </export>
      ```

   d. <!--PUPM COLLECTORS--> 섹션에서 다음 요소를 찾습니다.

      ```
      <export object="com.ca.ppm.export.ADGroupsCollector">
      </export>
      ```

   e. 다음과 같이 보이도록 이 요소를 편집합니다. 여기서 *ldap_query* 는 데이터가 수집된 대상 그룹을 정의하는 LDAP 쿼리를 지정합니다.

      ```
      <export object="com.ca.ppm.export.ADGroupsCollector">
              <where attr="%USER" satisfy="ANY">
                      <value op="EQUALS">(ldap_query)</value>
              </where>
      </export>
      ```

      Active Directory 스냅숏의 범위를 제한했습니다.

7. 새 스냅숏 매개 변수 XML 파일을 저장하고 닫습니다.

8. 새 스냅숏 매개 변수 XML 파일을 사용하도록 CA Access Control 엔터프라이즈 관리에서 스냅숏 정의를 수정합니다.

   캡처 스냅숏 작업이 실행되면 이 작업은 스냅숏 매개 변수 XML 파일에 지정한 데이터만 수집합니다.

예: 보고서 스냅숏의 범위를 CA Access Control 끝점으로 제한

PUPM 과 [assign the value for unab in your book]를 사용하지 않는 경우 CA Access Control 끝점에서만 데이터를 수집하도록 보고서 스냅숏의 범위를 제한할 수 있습니다. 데이터 수집의 범위를 CA Access Control 끝점으로 제한하려면 <-- PUPM COLLECTORS --> 섹션 아래에서 ReportIdMarkerCollector 항목을 *제외*한 모든 항목을 주석 처리(!-- 및 --)하십시오.

다음은 ReportIdMarkerCollector 항목을 제외하고 <-- PUPM COLLECTORS --> 섹션 아래의 모든 항목을 주석 처리하도록 수정된 이후의 PPM_ALL.xml 파일의 코드 조각입니다.

```
<!-- PUPM COLLECTORS -->
        <!-- export object="com.ca.ppm.export.AccountPasswordCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.PPMRolesCollector">
                <exportattr attr="|rolemembers|" />
        </export -->

        <!-- export object="com.ca.ppm.export.
                PrivilegedAccountExceptionCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.PPMPasswordPolicyCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.ADUsersCollector">
        </export -->

        <export object="com.ca.ppm.export.PPMAccountUserAccessCollector">
        </export --!>

        <!-- export object="com.ca.ppm.export.ADGroupsCollector">
                <exportattr attr="|groupmembers|" />
        </export -->

        <export object="com.ca.ppm.export.ReportIdMarkerCollector">
        </export>
```

스냅숏 매개 변수 XML 파일 구문 - 보고서 스냅숏 제한

스냅숏 매개 변수 XML 파일은 CA Access Control 엔터프라이즈 관리가 수집하는 보고서 데이터를 지정합니다. 스냅숏 매개 변수 XML 파일을 편집하여 보고서 스냅숏의 범위를 제한할 수 있습니다.

CA Access Control 엔터프라이즈 관리는 스냅숏 매개 변수 XML 파일에 정의하는 조건을 충족하는 개체에 대해서만 보고서 데이터를 수집합니다. 파일의 각 수집기는 CA Access Control 엔터프라이즈 관리가 수집하는 여러 개체를 정의합니다.

각 수집기는 다음과 같은 구조를 갖습니다.

```
<export object=" ">
        <where attr=" " satisfy=" ">
                <value> </value>
        </where>
        <exportattr attr=" " />
</export>
```

참고: <where>, <value>, <exportattr> 요소는 선택 사항입니다.

각 수집기는 다음 요소를 포함하고 있습니다.

<export>

CA Access Control 엔터프라이즈 관리가 수집하는 개체 데이터를 나타냅니다. 예를 들어, <export> 요소는 CA Access Control 엔터프라이즈 관리가 사용자 데이터를 수집하도록 지정할 수 있습니다.

<export> 요소는 하나 이상의 <exportattr> 및 <where> 요소를 포함할 수 있으며, 이 요소를 사용하여 특정 조건을 충족하는 데이터만 수집할 수 있습니다. <exportattr> 또는 <where> 요소를 지정하지 않으면 CA Access Control 엔터프라이즈 관리는 개체에 대한 모든 데이터를 수집합니다.

<export> 요소는 개체 매개 변수만 가집니다.

<where>

<value> 요소에 의해 정의된 조건을 기준으로 수집된 데이터를 필터링합니다. <where> 요소는 하나 이상의 <value> 요소를 포함해야 합니다. 또한 필터를 구체화하기 위해 여러 개의 <where> 요소(OR 요소로 작동)를 지정할 수 있습니다.

다음 표에서는 <where> 요소에 대한 매개 변수를 설명합니다.

매개 변수	설명
attr	필터에서 사용할 특성을 나타냅니다.
satisfy	개체 또는 특성을 수집하기 위해 일부 또는 모든 값 평가를 충족해야 하는지 나타냅니다. ■ ALL - 특성 또는 개체가 모든 값 평가를 충족해야 합니다. ■ ANY - 특성 또는 개체가 하나 이상의 값 평가를 충족해야 합니다.

<value>

<where> 요소에서 특성 또는 개체를 수집하기 위해 충족해야 하는 조건을 정의합니다. <value> 요소에는 연산자(op) 매개 변수가 필요합니다. 연산자는 EQUALS 또는 CONTAINS 일 수 있습니다.

참고: 스냅숏 매개 변수 XML 파일의 <!--PUPM COLLECTORS--> 섹션에서 <value> 요소에 LDAP 구문을 사용할 수 있습니다. LDAP 구문은 Active Directory 에서 CA Access Control 엔터프라이즈 관리가 수집하는 사용자 및 그룹 데이터를 지정할 수 있게 해 줍니다.

<exportattr>

수집할 특정 특성을 나타냅니다. 수집하는 개체에 대한 하위 특성을 수집하려면 <exportattr> 요소를 사용하십시오. 예를 들어, <exportattr> 요소를 사용하여 사용자의 ID 만 수집할 수 있습니다.

<exportattr> 요소는 attr 매개 변수를 갖습니다.

다음 표에서는 <where> 요소 또는 <exportattr> 요소에서 개체가 사용할 수 있는 특성을 표시합니다.

개체	<where> 요소에서 사용할 수 있는 특성	<exportattr> 요소에서 사용할 수 있는 특성
role	이름 특성으로 필터링할 수 있습니다. name - 필터를 충족하는 이름의 역할	다음 특성을 수집할 수 있습니다. ■ |tasks| - 역할과 관련된 모든 태스크 ■ |rules| - 역할에 적용되는 모든 구성원, 관리자, 소유자 및 범위 규칙 ■ |users| - 역할의 모든 구성원, 관리자 및 소유자 ■ |rolemembers| - 모든 역할 구성원 ■ |roleadmins| - 모든 역할 관리자 ■ |roleowners| - 모든 역할 소유자
사용자	잘 알려진 특성 또는 물리적 특성 및 다음 특성: ■ |groups| - 그룹의 구성원 ■ |roles| - 역할의 구성원 ■ |orgs| - 필터를 충족하는 조직에 프로필이 있는 사용자	다음 특성을 수집할 수 있습니다. ■ |all_attributes| - 사용 가능한 모든 사용자 특성 ■ |groups| - 사용자가 구성원 또는 관리자로 있는 모든 그룹 ■ |roles| - 사용자가 구성원, 관리자 또는 소유자로 있는 모든 역할

개체	<where> 요소에서 사용할 수 있는 특성	<exportattr> 요소에서 사용할 수 있는 특성
그룹	잘 알려진 특성 또는 물리적 특성 또는 다음 특성: |groups| - 필터를 충족하는 그룹 내 중첩된 그룹 목록	잘 알려진 특성 또는 물리적 특성 또는 다음 특성을 수집할 수 있습니다. ■ |all_attributes| - 디렉터리 구성 파일(directory.xml)에 그룹 개체에 대해 정의된 모든 특성 ■ |groups| - 그룹 내 중첩된 모든 그룹 ■ |users| - 그룹의 모든 구성원 ■ |groupadmins| - 지정된 그룹의 관리자인 모든 사용자 ■ |groupmembers| - 지정된 그룹의 구성원인 모든 사용자 ■ |users| - 모든 그룹 관리자 및 구성원
organization	잘 알려진 특성 또는 물리적 특성	잘 알려진 특성 또는 물리적 특성 또는 다음 특성을 수집할 수 있습니다. ■ |all_attributes| - 디렉터리 구성 파일(directory.xml)에 조직 개체에 대해 정의된 모든 특성 ■ |orgs| - 조직 내 중첩된 모든 조직 ■ |groups| - 조직의 모든 그룹 ■ |users| - 조직의 모든 사용자

LDAP 쿼리가 보고서 스냅숏에서 사용자 및 그룹 데이터를 제한하는 방법

사용자 저장소로 Active Directory 를 사용하는 경우 보고서 스냅숏에 캡처된 사용자 및 그룹 데이터를 지정할 수 있습니다.

사용자 및 그룹으로 Active Directory 데이터를 필터링하는 LDAP 쿼리를 스냅숏 매개 변수 XML 파일에서 사용할 수 있습니다. 하지만 역할 구성원 자격으로 Active Directory 데이터를 필터링하는 LDAP 쿼리를 사용할 수는 없습니다. LDAP 쿼리는 스냅숏 매개 변수 XML 파일의 <!--PUPM COLLECTORS--> 섹션에서만 사용할 수 있습니다.

다음 프로세스는 스냅숏 매개 변수 XML 파일의 LDAP 쿼리가 CA Access Control 엔터프라이즈 관리가 수집하는 Active Directory 데이터를 제한하는 방법을 설명합니다. 이 정보는 보고서 스냅숏을 제한하기 위해 올바른 LDAP 쿼리를 작성하는 데 도움을 줍니다.

CA Access Control 엔터프라이즈 관리가 Active Directory 보고서 스냅숏을 캡처할 때는 다음을 수행합니다.

1. 다음 요소 내에서 LDAP 쿼리에 지정된 Active Directory 사용자에 대해서만 데이터를 수집합니다.

   <export object="com.ca.ppm.export.ADUsersCollector">

   요소에 LDAP 쿼리가 없으면 CA Access Control 엔터프라이즈 관리는 스냅숏에 모든 Active Directory 사용자에 대한 데이터를 포함합니다.

2. 다음 요소 내에서 LDAP 쿼리에 지정된 Active Directory 그룹에 대해서만 데이터를 수집합니다.

   <export object="com.ca.ppm.export.ADGroupsCollector">

   요소에 LDAP 쿼리가 없으면 CA Access Control 엔터프라이즈 관리는 스냅숏에 모든 Active Directory 그룹에 대한 데이터를 포함합니다.

   참고: CA Access Control 엔터프라이즈 관리는 1 단계에서 쿼리에 의해 반환되지 않은 모든 사용자에 대해 데이터를 수집하지 않습니다. 사용자가 2 단계에서 쿼리에 의해 반환된 그룹의 구성원이지만 사용자가 1 단계에서 쿼리에 의해 반환되지 않았으면 CA Access Control 엔터프라이즈 관리는 Active Directory 스냅숏에 사용자에 대한 어떠한 데이터도 포함하지 않습니다.

LDAP 구문 고려 사항

Active Directory 스냅숏의 범위를 제한하기 위해 LDAP 쿼리를 작성할 때는 다음 사항을 고려하십시오.

- LDAP 쿼리에 다음과 같은 논리 연산자를 사용할 수 있습니다.
  - EQUAL TO (=)
  - OR (|)
  - AND (&)

    참고: 앰퍼샌드(&) 문자의 사용에는 일부 제한이 적용됩니다.
  - NOT (!)
  - 와일드카드(*)
- 앰퍼샌드(&) 문자 및 왼쪽 꺾쇠 괄호 문자(<)는 다음 구문에서만 사용할 수 있습니다.
  - 태그 구분 기호로 사용
  - 주석 내에서 사용
  - 프로세싱 지침 내에서 사용
  - CDATA 섹션 내에서 사용

다른 구문에서 앰퍼샌드 문자를 나타내려면 문자열 **&** 또는 유니코드 문자 참조를 사용하십시오. 다른 구문에서 왼쪽 꺾쇠 괄호 문자를 나타내려면 문자열 **<** 또는 유니코드 문자 참조를 사용하십시오.

- 오른쪽 꺾쇠 괄호 문자(>)는 CDATA 섹션( ]]>)의 끝을 표시하는 문자열 뒤에만 사용할 수 있습니다.

  다른 구문에서 오른쪽 꺾쇠 괄호 문자를 나타내려면 문자열 **>** 또는 유니코드 문자 참조를 사용하십시오.

예: 앰퍼샌드 문자

스냅숏 매개 변수 XML 파일의 다음 코드 조각은 보고서 스냅숏에 모든 Active Directory 사용자 데이터를 포함하도록 지정합니다. 스냅숏의 LDAP 쿼리는 & 문자열을 사용하여 앰퍼샌드를 나타냅니다.

```
<export object ="com.ca.ppm.export.ADUsersCollector">
        <where attr="%USER%" satisfy="ANY">
                <value op="EQUALS">(&amp;(objectClass=user))</value>
        </where>
</export>
```

제 5 장: CA Access Control for Virtual Environments REST API

이 섹션은 다음 항목을 포함하고 있습니다.

REST-based API

REST(Representational State Transfer)는 URL 에서 액세스 가능한 개체의 상태를 만들고 수정하기 위해 하이퍼미디어의 내재 속성에 의존하는 소프트웨어의 아키텍처 스타일 특성을 기술합니다.

REST 시나리오에서 문서(개체의 상태를 나타냄)는 클라이언트와 서비스 모두 단일 요청 또는 응답 내용 이외에는 어떠한 엔터티에 대해서도 아는 것이 없다고 가정 하에 이 둘 사이에서 주고받기됩니다.

REST 기반 API 에 대한 스키마를 얻으려면 다음 URL 을 탐색하여 빈 페이지에서 소스를 열어 보십시오.

https://*hostname*:18443/iam/api/1.0/restapi/schemas

참고: 스키마에 대한 자세한 내용은 이 섹션의 설명을 참조하십시오.

REST-based 인증

CA Access Control for Virtual Environments REST 요청은 요청 정보의 일부로서 인증 정보를 포함합니다. CA Access Control for Virtual Environments 는 HTTP 기본 인증 방법을 지원합니다. 예를 들어, 다음과 같은 기본 인증을 사용할 수 있습니다.

Authorization: Basic c3VwZXJhZG1pbjpkZWZhdWx0c3VwZXJhZG1pbjpkZWZhdWx0

위의 예제는 사용자 “superadmin” 및 암호 “default”의 Base 64 인코딩을 나타냅니다.

태그 가져오기

모든 태그의 목록을 보려면 GET 명령을 사용하여 모든 태그를 가져오십시오.

HTTP GET 요청을 다음 URL 로 보내십시오.

https://*hostname*:18443/iam/api/1.0/restapi/environment/ac/tags

특정 태그를 검색하려면 다음과 같이 GET 명령을 사용하여 태그 이름을 지정하십시오.

HTTP GET 요청을 다음 URL 로 보내십시오.

https://*hostname*:18443/iam/api/1.0/restapi/environment/ac/tags/<tag_name>

태그 만들기

POST 명령을 사용하여 태그를 만듭니다.

HTTP POST 요청을 다음 URL 로 보내십시오.

https://*hostname*:18443/iam/api/1.0/restapi/environments/ac/tags

태그를 만들려면 HTTP 본문에 다음 정보가 포함되어 있어야 합니다.

```
<Tag>
 <Name>태그 이름</Name>
 <Description>태그 설명</Description>
</Tag>
```

<Name>

태그 이름을 지정합니다.

<Description>

태그에 대한 설명을 지정합니다.

태그 수정

관리되는 장치에서 태그를 할당 또는 제거하기 위해 태그를 수정합니다.

Follow these steps:

1. GET 명령을 사용하여 태그 상태를 검색합니다.

   https://*hostname*:18443/iam/api/1.0/restapi/environments/ac/<tag_name>

   다음과 유사한 응답 XML 문서가 반환됩니다.

```
<Tag>
 <Name>testtag</Name>
 <Description />
 <Devices>
  device
   <ID>vm-11</ID>
  </Device>
 </Devices>
</Tag>
```

2. 수정된 태그를 사용하여 장치를 업데이트합니다.

   HTTP PUT 명령을 다음 URL 로 전달하십시오.

   https://*hostname*:18443/iam/api/1.0/restapi/environments/ac/<tag_name>

태그 삭제

태그를 삭제하려면 DELETE 명령을 사용하십시오.

HTTP DELETE 요청을 다음 URL 로 보내십시오.

https://*hostname*:18443/iam/api/1.0/restapi/environments/ac/tags/</*tag_name*>

관리되는 장치 태깅

컴퓨터를 보안 그룹에 추가하고 원격으로 관리하기 위해 관리되는 장치에 태그를 지정할 수 있습니다.

Follow these steps:

1. 관리되는 장치에 대해 CA Access Control for Virtual Environments 가 사용하는 ID 를 가져옵니다.

   관리되는 장치에 대해 CA Access Control for Virtual Environments 가 사용하는 ID 를 가져오려면 필터를 통해 장치 정보를 가져오도록 REST 요청을 사용하십시오. 예:

   https://*hostname*:18443/iam/api/1.0/restapi/environments/ac/devices?managed-object-vcenter-uuid=54E79C3A-49D5-4958-A983-8B919F470CEC&managed-object-id=vm-394

   참고: 앞의 예제에서 필터링 매개 변수로서 VMware Managed Object Browser(MOB)에 정의된 대로 vCenter UUID 와 VM UUID 를 전달합니다.

   다음과 유사한 응답 XML 문서가 반환됩니다.

```
<Devices>
 device
  <ID>vm-19</ID>
  <ParentID>esx-3</ParentID>
  <Name>ESXi in a box</Name>
  <Type>VirtualMachine</Type>
  <VirtualMachineProperties>
   <ManagedObjectID>vm-394</ManagedObjectID>

<ManagedObjectVCenterUUID>54E79C3A-49D5-4958-A983-8B919F470CEC</ManagedObjectVCenterUUID>
   <GuestOSVersion>LINUX_REDHAT_5</GuestOSVersion>
   <GuestOSArchitecture>X86</GuestOSArchitecture>
   <GuestOSDescription>Red Hat Enterprise Linux 5 (64-bit)</GuestOSDescription>
  </VirtualMachineProperties>
  <SecurityGroups>
   <SecurityGroup>
    <ID>sg-13</ID>
    <Name>weiig01esxi01.ca.com</Name>
    <Description/>
    <Owner>superadmin</Owner>
   </SecurityGroup>
   <SecurityGroup>
    <ID>sg-15</ID>
    <Name>Discovered virtual machine</Name>
    <Description/>
    <Owner>superadmin</Owner>
   </SecurityGroup>
```

```
    <SecurityGroup>
     <ID>sg-22</ID>
     <Name>vSphere in a box</Name>
     <Description/>
     <Owner>superadmin</Owner>
    </SecurityGroup>
   </SecurityGroups>
  </Device>
</Devices>
```

장치의 ID 는 응답 XML 파일에 지정된 것처럼 **vm-19** 입니다.

2. 할당된 태그를 사용하여 장치를 업데이트합니다.

   HTTP PUT 명령을 다음 URL 로 전달하십시오.

   https://<host>:18443/iam/api/1.0/restapi/environments/ac/devices/<*managed_device_ID*>

   참고: HTTP 내용에는 장치의 모든 기존 속성과 함께 새로 할당된 태그 정보가 포함되어 있어야 합니다. 기존 속성을 가져오려면 장치의 CA Access Control for Virtual Environments ID 에 대해 필터링했을 때 응답 XML 파일의 device…</Device> 태그 사이에서 데이터를 복사하십시오.

   새 태그 관계를 갖는 HTTP 내용의 예:

```
device
 <ID>vm-19</ID>
 <ParentID>esx-3</ParentID>
 <Name>ESXi in a box</Name>
 <Type>VirtualMachine</Type>
 <VirtualMachineProperties>
  <ManagedObjectID>vm-394</ManagedObjectID>
  <ManagedObjectVCenterUUID>54E79C3A-49D5-4958-A983-8B919F470CEC</ManagedObjectVCenterUUID>
  <GuestOSVersion>LINUX_REDHAT_5</GuestOSVersion>
  <GuestOSArchitecture>X86</GuestOSArchitecture>
  <GuestOSDescription>Red Hat Enterprise Linux 5 (64-bit)</GuestOSDescription>
 </VirtualMachineProperties>
 <Tags>
  <Tag>
   <Name>testtag</Name>
   <Description>testtag2 description</Description>
  </Tag>
 </Tags>
 <SecurityGroups>
  <SecurityGroup>
   <ID>sg-13</ID>
   <Name>weiig01esxi01.ca.com</Name>
   <Description/>
   <Owner>superadmin</Owner>
  </SecurityGroup>
```

```
  <SecurityGroup>
   <ID>sg-15</ID>
   <Name>Discovered virtual machine</Name>
   <Description/>
   <Owner>superadmin</Owner>
  </SecurityGroup>
  <SecurityGroup>
   <ID>sg-22</ID>
   <Name>vSphere in a box</Name>
   <Description/>
   <Owner>superadmin</Owner>
  </SecurityGroup>
 </SecurityGroups>
</Device>
```

관리되는 장치에서 태그 제거

보안 그룹에서 제거하기 위해 관리되는 장치에서 태그를 제거할 수 있습니다.

Follow these steps:

1. 관리되는 장치에 대해 CA Access Control for Virtual Environments 가 사용하는 ID 를 가져옵니다.

   관리되는 장치에 대해 CA Access Control for Virtual Environments 가 사용하는 ID 를 가져오려면 필터를 사용하십시오. 예:

   https://*hostname*:18443/iam/api/1.0/restapi/environments/ac/devices?managed-object-vcenter-uuid=54E79C3A-49D5-4958-A983-8B919F470CEC&managed-object-id=vm-394

   참고: 앞의 예제에서 VMware Managed Object Browser(MOB)에 정의된 대로 vCenter UUID 와 VM UUID 를 전달합니다.

   다음과 유사한 응답 XML 문서가 반환됩니다.

```
<Devices>
 device
  <ID>vm-19</ID>
  <ParentID>esx-3</ParentID>
  <Name>ESXi in a box</Name>
  <Type>VirtualMachine</Type>
```

```
  <VirtualMachineProperties>
   <ManagedObjectID>vm-394</ManagedObjectID>

<ManagedObjectVCenterUUID>54E79C3A-49D5-4958-A983-8B919F470CEC</ManagedObjectVCenterUUID>
   <GuestOSVersion>LINUX_REDHAT_5</GuestOSVersion>
   <GuestOSArchitecture>X86</GuestOSArchitecture>
   <GuestOSDescription>Red Hat Enterprise Linux 5 (64-bit)</GuestOSDescription>
  </VirtualMachineProperties>
  <SecurityGroups>
   <SecurityGroup>
    <ID>sg-13</ID>
    <Name>weiig01esxi01.ca.com</Name>
    <Description/>
    <Owner>superadmin</Owner>
   </SecurityGroup>
   <SecurityGroup>
    <ID>sg-15</ID>
    <Name>Discovered virtual machine</Name>
    <Description/>
    <Owner>superadmin</Owner>
   </SecurityGroup>
   <SecurityGroup>
    <ID>sg-22</ID>
    <Name>vSphere in a box</Name>
    <Description/>
    <Owner>superadmin</Owner>
   </SecurityGroup>
  </SecurityGroups>
 </Device>
</Devices>
```

장치의 ID 는 응답 XML 파일에 지정된 것처럼 **vm-19** 입니다.

2. 다음과 같이 장치를 업데이트하고 태그를 제거합니다.

   a. 1 단계에서 응답 XML 파일을 편집하고 <Tags>...</Tags> 태그 사이의 모든 내용을 제거합니다.

   b. HTTP PUT 명령을 사용하여 업데이트된 XML 파일을 다음 URL 로 보냅니다.

      https://<host>:18443/iam/api/1.0/restapi/environments/ac/devices/vm-19

예제: HTTP 스키마

다음은 지원되는 REST 기반 API 명령의 스키마 예제입니다.

- HTTP POST:

```
POST /iam/api/1.0/restapi/environments/ac/tags HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 79

<Tag><Name>testtag</Name><Description>testtag2 description</Description></Tag>
```

- HTTP GET:

```
GET /iam/api/1.0/restapi/environments/ac/devices/vm-19 HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.169:9998
```

- HTTP PUT:

```
PUT /iam/api/1.0/restapi/environments/ac/devices/vm-19 HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 959

<Devices>device<ID>vm-19</ID><ParentID>esx-3</ParentID><Name>ESXi in a
box</Name><Type>VirtualMachine</Type><VirtualMachineProperties><ManagedObjectID>vm-394</ManagedObj
ectID><ManagedObjectVCenterUUID>54E79C3A-49D5-4958-A983-8B919F470CEC</ManagedObjectVCenterUU
ID><GuestOSVersion>LINUX_REDHAT_5</GuestOSVersion><GuestOSArchitecture>X86</GuestOSArchitecture
><GuestOSDescription>Red Hat Enterprise Linux 5
(64-bit)</GuestOSDescription></VirtualMachineProperties><Tags><Tag><Name>testtag</Name><Description>testt
ag2
description</Description></Tag></Tags><SecurityGroups><SecurityGroup><ID>sg-13</ID><Name>weiig01esxi01.
ca.com</Name><Description/><Owner>superadmin</Owner></SecurityGroup><SecurityGroup><ID>sg-15</ID><
Name>Discovered virtual
machine</Name><Description/><Owner>superadmin</Owner></SecurityGroup><SecurityGroup><ID>sg-22</ID><
Name>vSphere in a
box</Name><Description/><Owner>superadmin</Owner></SecurityGroup></SecurityGroups></Device></Devices
>
```

- HTTP DELETE:

```
DELETE /iam/api/1.0/restapi/environments/ac/tags/testtag HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```